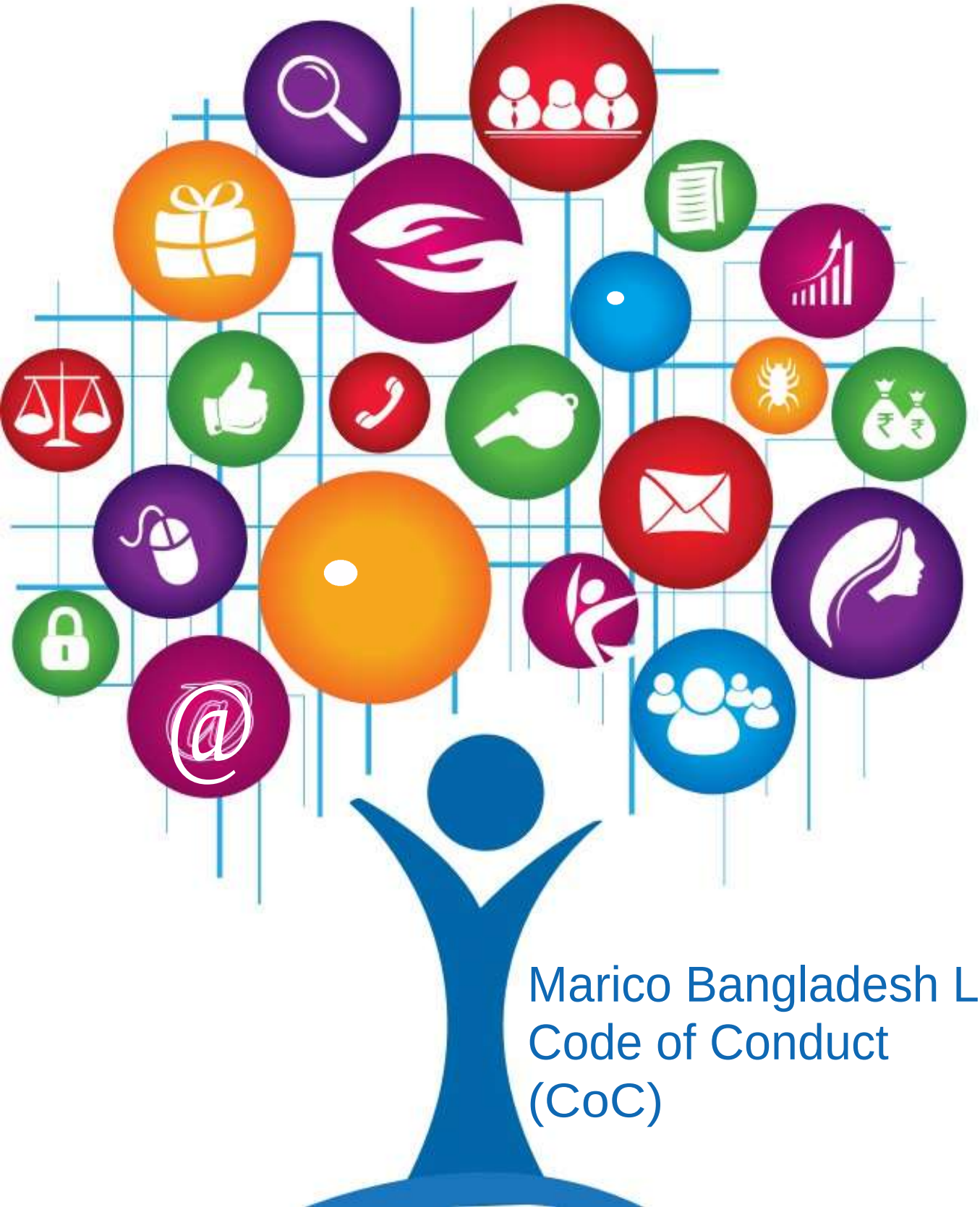

Marico Bangladesh Limited
Code of Conduct
(CoC)

MARICO BANGLADESH LIMITED
Code Of Conduct

This Code of Conduct is adapted from the Code of Conduct of Marico Limited which is the unified code applicable to all subsidiaries within the Marico group. The Code was originally adopted by the Board of Directors of Marico Limited on 1st November 2010. The First Amendment to the Code was adopted on 25th March 2014

This Code of Conduct will be known as Marico Bangladesh Limited Code of Conduct (Hereinafter to be referred to as "the Code/this Code"). This Code is applicable to all Members.

For the purpose of this Code, the following terms will have the meaning assigned to it as hereunder, unless the context otherwise requires

1. "Member" means
i) a director (executive or non-executive) and an employee whether part-time or full-time, fixed term, permanent trainee of Marico Bangladesh Limited; or
ii) an individual who is a temporary staff, intern, secondee, an apprentice; or
iii) a third party or parties who represent the Company or act on behalf of the Company.
2. "Audit Committee" means the Committee of the Company constituted by the Board of Directors of the Company.
3. "Chairman" and "Managing Director" respectively means the Chairman and Managing Director (MD) of Marico Bangladesh Limited.
4. "Corporate Governance Committee" means the Committee of the Company constituted by the Board of Directors of the Company.
5. "Company" shall mean Marico Bangladesh Limited (MBL) a subsidiary of Marico Limited.
6. "Group" shall mean Marico Limited and all it's subsidiaries (hereinafter interchangeably referred to as Marico).
7. "Group Company" shall mean the parent and associated companies of Marico Bangladesh Limited
8. "Improper Activities" includes but is not limited to :
i) Questionable accounting, internal accounting controls or auditing matters
ii) Disclosures in documents filed by the Company with statutory authorities and other public disclosures made by the Company that may not be complete or accurate
iii) Fraudulent financial reporting
iv) Violation of any policies of the Company
v) Violation of laws applicable to the Company
vi) Fraud against company's shareholders
vii) Forgery or alteration of any documents
viii) Misappropriation or misuse of Company resources, such as funds, supplies or other assets;
ix) Pursuits of a benefit or advantage in violation of conflict of interest policy of the Company state herein above
x) Unauthorized alteration or manipulation of computer files
xi) Disclosure of confidential information without any authorization
xii) Any other act or omission which involves gross misconduct and / or violation of any provision of this Code

Guiding Principles

The underlying philosophy of this code is to conduct our business in an ethical manner as well as create a work environment that is conducive to members and associates alike, based on our values and beliefs.

To help us meet this commitment, the Code defines what we expect of our members and associates. This Code of Conduct sets out guidelines for each individual to follow.

The Code does not cover every eventuality or situation and the laws in each country also differ. Where you encounter situations not covered by the Code, always reflect on the spirit of the Code and values of MBL to make a decision based on common sense and good judgment. In case of any doubts, please consult with your supervisor and / or your HR Representative or any member of the Code of Conduct Committee.

The provisions of the Code shall be in addition to and not in derogation of the provisions of any other law for the time being in force. Where differences exist as the result of local customs, norms, laws or regulations, you may apply either the code or local requirements - whichever is more stringent and sets highest standards of recommended behaviour. Similarly where the Marico Group standards are more stringent those will supersede the provisions of this Code. In all cases local law or regulations will take precedence of the provisions of the Code or Group Code.

If compliance with the Code conflicts with any local laws and / or practices, please notify this immediately to the Code of Conduct Committee (CCC). The Code establishes principles for business conduct applicable in MBL and throughout the Group, regardless of location. The organization will support and stand by all decisions taken by Members in the spirit of trust and membership.

Business Integrity

Company Assets And Financial Integrity

Workplace Integrity

Your Responsibilities

GREVIENCE REDRESSAL MECHANISM

ANNEXURES

ACKNOWLEDGMENT / CONSENT FORM

Marico's Code of Conduct (CoC)

YOUR RESPONSIBILITIES
BUSINESS INTEGRITY

ALL IS NOT FAIR
... in the war at work!

BUSINESS INTEGRITY

i. Conflict of Interest

You shall act in the best interest of the Company at all times.

Conflicts of interest situations arise when Member's personal, social, financial or political activity conflicts with Member's objectivity at work or conflicts directly or indirectly with the interests of the Company.

Members shall not directly or indirectly:

a) Compete against the Company

b) Use their position or influence to secure an improper benefit for themselves or others.

c) Use Company information, assets or resources for their personal gain or the improper benefit of others

d) Take advantage of inside information or their position with the Company.

When any conflict of interest circumstances arise, or when there is doubt regarding possible conflict of interest, you shall disclose the same in writing with details to your immediate supervisor and / or your HR representative.

You shall not directly or indirectly:

- accept any simultaneous employment with suppliers, customers, competitors or engage in any activity that enhances or supports a competitor's position as this is a direct conflict of interest. Additionally, you shall disclose to immediate supervisor and your HR representative of any interest that you may have with the business of the Company.
- accept position as a Board Member in any other company without obtaining prior written approval from the Managing Director. (This does not apply to the non-Executive members of the Board of Directors of the Company)
- invest in a manner that may adversely affect your decision to make objective decisions on behalf of the Company. You shall immediately declare to your supervisor and HR representative about any "substantial interest" you may have or already have in any competitors, supplier or customer (substantial interest may be commonly understood as anything more than 1% of the stocks of a public company). However, if you have a discretionary authority in dealing with that company, any investment would be considered a conflict of interest.
- exploit, for personal gain, any opportunities that are discovered through the use of the Company's property, information or position, unless the opportunity is disclosed fully in writing to the Board of Directors and the Board declines to pursue such opportunities for the Company.

Further, you shall promptly disclose to your supervisor and HR representative any professional interaction with close relatives who could be prospective member, business associates, vendors, competitors where a situation of conflict of interest can arise. (Close Relative means spouse, partner, fiancé/ fiancée, parent, step-parent, child, step-child, sibling, step-sibling, nephew, niece, aunt, uncle, grandparent, grandchild and in-law).

Co-Member relationships

If you are or become involved in relationship with a co-Member then you shall discuss this issue with your immediate Supervisor and HR representative. Such issue shall be handled sensitively but it will be necessary to make changes to your working environment or reporting structure, including transferring one or both Members to avoid any conflict. Care should be taken proactively by the concerned Members that their behaviour towards each other does not cause discomfort to Members around.

ii. Receiving and giving Gifts and Entertainment

We believe that business relationships founded on trust and mutual interest are vital to our success. We believe in conducting ourselves honestly, responsibly and fairly in our interactions with everyone including our customers, contractors and suppliers.

a) Members should not accept any offers, payment, promise to pay any money, gift or anything of value from associate, customer, vendor, other members etc that is perceived as intended, directly or indirectly, to influence any business decision or any commitment of fraud.

b) Inexpensive gifts, infrequent business meals etc do not violate this Code provided they are not excessive or create an appearance of impropriety.

c) Gifts given by Members to business associates or received from them should be appropriate to the circumstances and should never create an impression of impropriety.

d) We would encourage members to build long-term relationships with suppliers, vendors etc. so as to derive business benefit in the long-term. Members should ensure that gifts or entertainment in this regard are appropriate to the circumstances.

Some examples of appropriate gifts:

- Meals: modest occasional meals with someone with whom we do business
- Entertainment: occasional attendance at ordinary sports, theatre and other cultural events
- Gifts: gifts of nominal value, such as pens, calendars, or small promotional items.

Some examples of gifts those are clearly inappropriate:

- Any gift or entertainment that would be illegal (against the law of the land)
- Gifts or entertainment involving parties engaged in a tender or competitive bidding process
- Any gift of cash or cash equivalent (such as gift certificates, loans, stock, stock options)
- Any gift or entertainment that is a 'quid pro quo' (offered for something in return)
- Any entertainment that is indecent, sexually oriented, does not comply with the organization's commitment to mutual respect or that otherwise might adversely affect its reputation.
- A gift or entertainment that you pay for personally to avoid having to report or seek approval for, a specific action.

You will use your own discretion to use the gifts received which are appropriate, due to your role in the Company, for / in the Company.

In case of any doubt and / or if unable to classify the gift received, you will seek guidance from the immediate supervisor and act appropriately.

In case an inappropriate gift is offered or received, you will return and / or intimate the same to the concerned party immediately, as is applicable in conjunction with this Code. You will also report the same to the immediate supervisor.

iii. Bribery

You will always encourage meritocracy and shall follow it as a principle while interfacing with others including other members, government officials, business associates, contractors, agents etc. Therefore, giving or receiving an undue reward / bribe or anything to influence the behaviour of someone to obtain commercial advantage is discouraged.

Please note that in Bangladesh, under the Prevention of Corruption Act 1947, the Penal Code 1860 and the Anti-Corruption Commission Act 2004 and rules/regulations framed thereunder giving of bribe to governmental officials and agents whether directly or indirectly, is strictly prohibited and amounts to a criminal offence. As a law abiding Member, you will not directly or indirectly pay any bribe to any other Members, Governmental officials, business associates, contractors, vendors, agents, etc.

iv. Working with Associates

MBL's associates play a critically important role in our ability to operate and provide products and services to our customers. That is why we must choose them carefully, based on merit, and with the expectation that our associates will act consistently with our compliance and ethics requirements.

a) You will choose an associate on merit; avoid conflicts of interest, inappropriate gifts and entertainment or any other kind of favouritism that might compromise or influence selection

b) You will seek to do business with associates who comply with legal requirements and who act in a manner that is consistent with MBL's commitment to compliance and ethics as outlined in this Code

c) You will help our associates understand our compliance and ethics requirements

d) You will always deal fairly, ethically and lawfully with associates and customers.

"Associate" is any external person / body of persons / company / organisation we do business with. They could be advertising agencies, distributors, consultants, vendors, suppliers, third party manufacturers, etc. A separate set of guiding principles governing our relationship with our associates, known as MBL Code of Business Ethics (MCOBE) is provided as an annexure to this Code of Conduct. This would be provided and signed-off during enlistment of Associates as vendors or during execution of an agreement with Associates and compliance with the same is mandatory for our continued association with such third parties. Any deviation in complying with MCOBE would be treated as a breach of this Code liable to terminate the relationship/arrangement or require appropriate legal proceedings.

Please note that additional rules regarding associates may apply to a particular job, you are expected to get such additional rules (if any) from your supervisor and / or HR representative.

v. Compliance with laws of the land

a) You will comply with all the applicable laws, regulations, rules and regulatory orders.
b) You will acquire appropriate knowledge of the requirements relating to your duties sufficient to enable you to recognise potential dangers and to know when to seek advice from your supervisors, HR representatives or Legal department on specific law or company policies and procedures.
c) Violation of any law, regulations, rules and orders may make you liable for criminal or civil action, in addition to any disciplinary action that the Company may take against you for such violation.
d) You will not at any time or under any circumstances enter into an agreement or understanding, written or oral, express or implied with any competitor concerning prices, discounts, other terms or conditions of sale, profit or profit margins, costs, allocation of products or geographic markets, allocation of customers, limitations on production, boycotts of customer or suppliers, or bids or the intent to bid or even discuss or exchange information on these subjects. These prohibitions are absolute and strict observance is required.

YOUR RESONSIBILITIES

COMPANY ASSETS CONFIDENTIALITY AND FINANCIAL INTEGRITY

Treat it like it belonged to you

... carefully

COMPANY ASSETS CONFIDENTIALITY AND FINANCIAL INTEGRITY

i. Accurate and complete data, records, reporting and accounting

You will provide to all stakeholders and other Members information that is correct and complete.

For example:

a. Financial data (e.g. books, records and accounts) must conform both to generally accepted accounting principles and to the Company's reporting policies

b. Information provided for employment records should be factual and accurate in all aspects.

In line with our values of trust and openness, we will be forthright and transparent about our operations and performance, accurate in the recording and reporting of data and results, and exercise care in the use of our assets and resources.

You will treat all information that is not in the public domain (not on the Company's annual / quarterly report, published in the internet / intranet) with care. Any information stated as confidential explicitly should be treated as such.

You will not misuse and / or misappropriate the funds of the Company in any manner.

For other information where there is a doubt, you will check with the immediate supervisor or HR representative. You will not use any confidential information of the Company to accrue personal gains.

You will use Claims Against Self Authorization (CEASE), where applicable, with responsibility and integrity. You are required to read and understand the CEASE guidelines available on Group intranet/ Mera Milaap or on any other platform made available by the Company to you.

ii. Usage of Company Assets

All members are responsible for using good judgment to ensure that organization assets are not misused or wasted.

Company assets includes all assets including but not limited to work stations, electronic devices / equipments, materials and resources, company's intellectual property rights, software, confidential / proprietary information, facilities like internet, air conditioning, toasters, beverage vending machines, etc.

You are responsible for the proper use of the Company assets at your disposal including those provided to you for the performance of your job / work by the Company. You must safeguard such properties / asset(s) against loss, damage, misuse or theft.

You agree to use the Company properties / asset(s) only for the purpose for which the same has been provided to you and not for any other purpose. You will ensure that the Company asset is not abused or wasted.

iii. Electronic Usage

You must utilize electronic communication devices made available to you in the manner in which such devices are meant to be used and for the purpose for which the same has been provided to you. You will be responsible for the fair and proper use of all electronic communications devices within the Company, including computers, e-mail, connections to the Internet, intranet and extranet and any other public or private networks, voice mail, video conferencing, facsimiles, and telephones. Posting or discussing information concerning the Company's products, services or business on the Internet without the prior written consent of the Supervisor, Head –Human Resources and Head – Legal is strictly prohibited. Any other form of electronic communication used by Members currently or in the future is also intended to be encompassed under this Code. It is not possible to identify every standard and rule applicable to the use of electronic communications devices. Members are therefore encouraged to use sound judgment whenever using any feature of our communications systems. For more details please read and understand MBL's Information Security Policy (Annexure IV).

iv. Insider trading

The Company follows a strict policy on Members' share dealing rules.
Please read and understand the "MARICO BANGLADESH LIMITED SHARE DEALING RULES FOR DIRECTORS AND EMPLOYEES (Annexure V) for greater details.
You shall at all times abide by the said Rules.

v. Confidentiality

Confidential information shall include but not be limited to all undisclosed financial data or information, strategic business plans, product architectures, source codes, product plans and road maps, proprietary and technical information, intellectual properties viz. trade secrets, trademarks, copyrights, patents, etc., employee details, list and names of suppliers, vendors, dealers, financial information and projections, price sensitive information, non-public information and such other information which will be specifically termed as “Confidential Information”.

Members shall at all time protect the Confidential Information and shall not disclose Confidential Information to any person.

vi. Information Security

In order to maintain, secure, and ensure legal and appropriate use of the Company’s information technology infrastructure, the members are required to follow, adhere to and comply with the Information Security Policy, forming part of this Code of Conduct (Annexure IV) and the Information and Communications Technology Act 2006.

YOUR RESONSIBILITIES
WORKPLACE INTEGRITY

MATTERS OF
THE HEART
... can cause flutters
at the workplace

WORKPLACE INTEGRITY

i. Equal Opportunity Workplace

MBL is committed to building a work environment of mutual trust, where all members are treated with dignity and respect. Members will be recruited, selected, developed, transferred and advanced basis our principle of meritocracy - requirements of the role and business.

You will treat all other Members of the MBL with dignity, courtesy, respect and with equality irrespective of race, colour, religion, gender identity, age, national origin, sexual orientation, marital status, physical disability, etc.

You will not abuse your position and influence other Members for committing any type of offence.

ii. Harassment-Free Workplace

MBL stands committed to maintaining a work environment free from all forms of harassment and discrimination for all members consistent with its commitment to conduct its business in accordance with principles of equality, equal opportunity, and human rights.

A key manifestation of a pleasant and conducive work environment is respect for the individual, irrespective of the gender, race, ethnicity, age, disability or religious orientation of the
member concerned. In order to sustain this strongly through creation of a better understanding, behaviours that go against mutual respect have been articulated.

Marico aims to:

- Promote appropriate standards of conduct at all times
- Encourage the reporting of behavior which breaches the Guidelines on Prevention of Sexual Harassment
- Provide an effective procedure for complaints based on the principles of natural justice
- Treat all complaints in a sensitive, fair, timely and confidential manner
- Guarantee protection from any victimization or reprisals
- Implement training and awareness - outlining strategies to ensure that all members and associates know their rights and responsibilities.

Create a working and learning environment that is free from harassment and where all individuals associated with MBL are
treated with dignity, courtesy and respect

You will never indulge in any act which is inconsistent with the principles of equality, equal opportunity and human rights.

You will read, understand and abide by the Prevention of Sexual Harassment at Workplace Policy annexed with this Code marked as Annexure I.

iii. Abuse - Substance or Alcohol

You will not use or be in possession or under influence of alcohol or illegal drugs or any other controlled / prohibited substance / material in the work place on the job or during working hours.

In case you need to use / possess any such substance under medical prescription, then you shall immediately inform your Supervisor and HR representative.

iv. Abuse of Position / Designation - Bullying

You will not abuse your position in the Company to gain any illegal advantage or for committing any offence.

Bullying is unreasonable behaviour that is directed against an individual or group; by another individual or group and is derived from the misuse of power over the target of the behaviour. This may include:

- verbal abuse, shouting
- excluding or isolating behaviour
- deliberately withholding information vital for effective work performance
- giving employees impossible assignments
- physical abuse.

It is the responsibility of all Members to ensure that premises and facilities are free from harassment, every Member has a responsibility to meet this requirement.

Bullying is unreasonable behaviour derived from misuse of power. It is unacceptable conduct and all reported incidents will be investigated

v. Racial and Religious Vilification

Racial and religious vilification is conduct that incites hatred against, serious contempt for, or revulsion or severe ridicule against a person or group on the grounds of racial identification or religious belief or activity. Racial and religious vilification is a form of harassment and discrimination and is unacceptable conduct in the Company.

vi. Respecting Privacy & Confidentiality of Members

You are expected to respect the privacy of other Members and safeguard the confidentiality of information that MBL, Marico or you had about such member. You shall comply with any and all local and international privacy and data protection laws or guidelines :

a) Information pertaining to a member must be obtained only with prior consent of such Member;
b) Members personal information gathered must be reasonable, relevant and not be intrusive in relation to the purpose for which it is collected. Such information shall only be used for the purpose for which it is collected and shall not be retained longer than necessary.
c) All member personal information shall be kept confidential and secure.
d) Advice must always be sought from the Head of Legal before gathering any personal information of a member or moving such information gathered outside the country of origin.

vii. Dress Code

Members are expected to dress appropriately during working hours or when representing the Organisation. This means presenting yourself in a professional, business appropriate style at all times. In addition you must ensure that your attire does not present a safety issue.

viii. Internet Social Media Policy

You shall not represent the Company or any brand of the Company without prior written approval from your Supervisor, Head of such Brand or Head of Legal in any blog site, social networking site, micro blog sites, photo / video sharing sites, chat rooms, chatting sites or alike. You will also adhere to the Information Security Policy in this connection.

GRIEVANCE REDRESSAL MECHANISM

SPEAK UP - Today

before it's too late!

GRIEVANCE REDRESSAL MECHANISM

1. Various contact points

If you have a question or concern about legal or ethical standards, you can choose to reach out to multiple members in the Company who will be equipped to help you resolve your concern. You have the following options for reaching out.

1) Complaint Drop Box - installed at all MBL locations
2) Email your query or complaint at - speakupmarico@ethicshelpline.in
3) MBL Website www.marico.com/bangladesh
5) Personally contact - any Member of the MBL Code of Conduct Committee

The access to Complaint drop box, email, complaints lodged through the MBL Website will be with the MBL CCC

6) Your Line management is usually a good place to start with a legal or business conduct issue who shall inform the Code of Conduct Committee (CCC).
7) Your HR representative who shall inform the Code of Conduct committee.

In case of a concern on Sexual harassment, in addition to the above touch points, you also have the option of contacting any member of the PoSH (Prevention of Sexual Harassment) Committee. The names of the members are mentioned in Annexure II.

If you observe behaviour that concerns you, or that may represent a violation of the Code or any law, raise the issue promptly. Doing so will allow the Company an opportunity to deal with the issue and correct it, ideally before it becomes a violation of law, security or the Company's reputation.

2. Administration and Governance of the Code

2.1 The Company has constituted a Committee which will also be known as the "Code of Conduct Committee" ("CCC").

2.2 Members to CCC will be appointed in the manner as specified under Annexure II.

2.3 CCC will have one Sub-committee namely Prevention of Sexual Harassment Committee (PoSHC). The objective of this committee is to administer the PoSH policy in providing a harassment free work environment including but not limited to appointment of investigation team for investigation of a complaint.

3. Role and functions of Prevention of Sexual Harassment Committee

3.1 PoSHC will primarily deal with complaints / concerns relating to sexual harassment at the workplace.

3.2 CCC on receiving complaint related to sexual harassment or if CCC has reason to believe that there is any incident of sexual harassment, then it will promptly divert such complaints to PoSHC.

3.3 The PoSHC may also receive complaints / concerns relating to sexual harassment directly or indirectly.

3.4 PoSHC shall report to the CCC.

3.5 All complaints / concerns shall be recorded and will be submitted to CCC before the quarterly meetings of CCC or as and when called for by the CCC.

3.6 PoSHC will also be responsible for adhering to the compliance requirements as per the PoSH Policy in overseeing conciliation, training and cascading and filing of statutory returns to the government authorities, as may be applicable.

4. Broad Principles of CCC

CCC along with its sub-committees will operate on the following principles:

a) Confidentiality,
b) Impartiality,
c) Promptness,
d) Sensitivity,
e) Courtesy and
f) Respect

5. Reporting of Grievances & Redressal

Until the formation of a Corporate Governance Committee under the Board of Directors, the CCC will report directly to the Audit Committee of the Company.

All sub-committees under CCC shall report to CCC.

The Company Secretary or the Chief Financial Officer shall be responsible to submit/file such reports/forms/returns as may be directed by the Government from time to time under any law for the time being in force.

6. Responsibilities of CCC

6.1 Administering, implementing and overseeing ongoing compliance under the Code.

6.2 Establishing, amending where necessary and administering procedures to assure that reports of Improper Activities will be collected, reviewed promptly, treated or resolved in an appropriate manner, and retained.

6.3 Making himself or herself available to discuss with Member(s) any complaints raised or reports filed personally with such CCC Member or otherwise.

6.4 Notifying the sender and acknowledge receipt of the reported violation or suspected violation. All reports will be promptly investigated and appropriate corrective action shall be taken.

6.5 Establishing, amending wherever necessary and administering procedures that enable Member(s) to submit reports of Improper Activities and related concerns in a confidential or anonymous manner.

6.6 Ensuring that the Members who are responsible for preparing and reviewing the Company's statutory filings and other public disclosures are made aware of reports of Improper Activities involving the Company's accounting, auditing, and internal auditing controls or disclosure practices.

6.7 Convene periodic training programs / workshops for all Members across all locations to educate them and to keep them updated with any new external development / amendments / changes in connection with the Code / applicable Laws.

6.8 In case any Member of a sub-committee has reason to believe that there is any violation of the Code / law, then in such situation, such Member should promptly inform in writing any Member of CCC or CFO of such incident and then after obtaining directions of CCC, conduct investigation.

6.9 Provide directions, instructions and assistances to all sub-committees.

Other Responsibilities:

CCC shall submit its quarterly report along with summary of all meetings held, all pending Code investigations and final Code decisions, including disciplinary actions shall be taken to the Audit Committee, until the formation of the Corporate Governance Committee, and thereafter shall be taken to the Corporate Governance Committee and Audit Committee of the Company.

CCC will also use representative samples of Code violations, while protecting the identity and privacy of the individuals involved, at the time of conducting awareness sessions for members.

7. Modifications

CCC shall continuously review and update this Code and procedures. Any amendment of this code or any decision to exempt the application of any part of the code to any section of the Company - must be approved in writing by the Corporate Governance Committee of MBL's Board of Directors and promptly disclosed on the Company's website and in applicable regulatory filings pursuant to applicable laws and regulations, together with details about the nature of the amendment or waiver. The CCC may, upon application by any Member or Suo moto issue any clarifications in respect of the code. Such clarifications shall be binding on the Company and the member. All clarifications issued shall operate prospectively and retrospectively unless expressly stated otherwise in such clarification.

8. Meetings of CCC

8.1 CCC shall meet as and when necessary, but at least four times in a year; ideally at the start of each quarter to review / report matters / issues of the last quarter.

8.2 Proceedings of all meetings shall be recorded within ten (10) days of the meeting. Such recorded proceedings will be available with the Secretary of CCC.

8.3 Proceeding of such meeting will be reviewed and submitted to the Audit Committee (until formation of the Corporate Governance Committee) of MBL.

8.4 All records of investigation / proceedings / records pertaining to any case / complaint will be kept confidential.

8.5 Records will be maintained by the Secretary of the CCC.

8.6 Only Members of CCC, Audit Committee, or as applicable Corporate Governance Committee, and Board of Directors will have access to such records and none.

9. Quorum of CCC Meeting

9.1 Presence of 2(two) members of CCC will be required for any decisions regarding selection of investigating committee or for the presentation of findings of investigation or for deciding any case about any Code violation.

9.2 Any Member of CCC absent without any valid reason for more than three consecutive times for the CCC meetings may be removed and new Member may be appointed by the remaining CCC Members.

10. Maintenance of case files, records and reports

a) All cases investigated under this Code will be maintained in a file and will be serially numbered.

b) Each case will carry a formal closure report, which will be signed by the Chairman of CCC within 30 (thirty) days of deciding the case.

c) All case papers, investigation reports with case closure report will be physically filed with the Secretary of the CCC.

d) There will be an electronic storage folder shared amongst the CFO, MD and Head-HR. This location shall carry e-copies of the papers physically filed with the Secretary of the CCC pertaining to all cases under this Code.

e) Only the following 3 individuals shall have access to the physical or electronic copies

i. MD
ii. CFO
iii. Head HR

f) This said system of record keeping and maintaining will be periodically audited, without such auditor getting into the contents of cases.

11. Anonymity and Confidentiality

CCC will not distinguish between any complaint / issues raised anonymously and those raised with identity disclosed.

When you report any non-compliance, violation or any complaint to the CCC through any medium, you may choose to remain anonymous, although you are encouraged to identify yourself to facilitate investigation / communication.

If you make your identity known, the Committee and investigators will keep your identity confidential, consistent with conducting a thorough and fair investigation.

In case you complain / raise any issue anonymously, attempt will nevertheless be made to seek details from the anonymous complainant

CCC will not make any effort to attribute the identity of the anonymous complainant to any Member.

12. Investigations

All complaints that make out a prima facie case of violation of the Code shall be investigated. The Company may handle the investigation internally or engage expert investigators.

CCC takes all reports of possible misconduct / violation of law / Code seriously. CCC will investigate the matter confidentially, make a determination whether the Code or any law has been violated, and take appropriate corrective action.

While conducting an Investigation following any complaint, CCC will ensure it adheres to the Principles of Natural Justice namely:

i. Both parties shall be given reasonable opportunity to be heard along with witnesses and to produce any other relevant documents

ii. No Person will be allowed to be a judge in his / her own case

iii. The final decision will be made after due investigation and the application of proper reasoning.

iv. The order of the CCC shall be in writing and shall contain reasons for arriving at the decision.

Upon completion of the investigation, both parties (if the identity of the complainant is known) will be informed of the decision of the CCC.

No set of rules can cover all circumstances. These guidelines may be varied as necessary to conform to local law or contract.

13. Detailed description of the Investigation Process

13.1 Gathering concerns/queries/complaints:

- Member can address a concern or query to multiple touch points. The Company is open to listen to its members at all times.
- On receiving any complaint / concern, the CCC will need to judge the concern:
  - i) If the concern does not have anything to do with this Code of Conduct, literally and in spirit, the office of the CCC will refer it to the appropriate authority that can solve the issue. E.g.: Payroll-related concerns, administration-related concerns etc.
  - ii) If the concern is related to the Code of Conduct, the office of the CCC will immediately initiate the investigation process.

All concerns regarding code violation will be directed to the Chairperson of CCC, irrespective of who receives it. Care will be taken that the first person who receives the concern does not exercise personal Judgement regarding the same.

13.2 Constitution of Investigation team

CCC will investigate complaints itself or may constitute an appropriate investigation team, depending upon the type of complaint; within 2 weeks of receiving the complaint.

CCC will not decide any matter without thorough investigation, except

on some cases where the misconduct / breach / violation of the Code or any law is apparent or the offender / defendant confesses about such misconduct / breach / violation of the Code or any law.

Investigation team may differ depending upon the type of complaint received by CCC.

14. Decision of CCC

14.1 CCC Members shall decide the cases about any Code violations.

14.2 Decision of CCC shall be final and binding upon the Members involved in a particular case.

14.3 CCC shall provide reasoning to its decision.

14.4 Presence of minimum 2(two) members of CCC will be considered valid for any decisions regarding selection of investigating committee or for the presentation of findings of investigation or for deciding any case about any Code violation.

14.5 In the event of any dissent within the CCC on any decision, the decision of the majority shall prevail. In the event of equal number of votes cast for and against a decision, there shall be re-voting. In the event that the re-voting also results in equal number of votes cast for and against the decision, the Chairman of the CCC shall have a casting vote.

14.6 CCC will table its findings to the Audit Committee, or as applicable the Corporate Governance Committee, every quarter.

15. Disciplinary Actions

CCC strives to impose discipline that fits the nature, gravity and circumstances of each Code violation. It uses a system of progressive discipline, issuing letters of reprimand for less significant, first-time negligent offenses. Violations of a more serious nature may result in transfer, suspension without pay; loss or reduction of merit increase, bonus or stock option award; or termination of employment without compensation. The complainant's views may be taken into consideration for this purpose.

i) No Retaliation

The Company has an unwavering policy against retaliation for raising a good-faith concern under this Code. The Company values the help of members or associates who follow this Code of Conduct and raises a concern or reports misconduct / violation. Any retaliation against a member or organization that raises an issue honestly is a violation of this Code. That a member has raised a concern honestly, or participated in an investigation, cannot be in any circumstances, the basis for any adverse employment action, including separation, demotion, suspension, loss of benefits, threats, harassment or discrimination.

The Company has an unwavering policy against retaliation. Any retaliation against a member or organisation that raises an issue honestly is a violation of this code.

Allegations of retaliation will be investigated and appropriate action will be taken. Anyone responsible for reprisals against individuals who report suspected misconduct or other risks to business will be subjected to disciplinary action up to and including dismissal.

If you believe someone has retaliated against you, or if you suspect that you or someone you know has been retaliated against for raising an ethical issue report the matter immediately to the Ethics Committee.

ii) Making False Accusations

Honest reporting does not mean that you have to be right when you raise a concern; you just have to believe that the information you are providing is accurate. Knowingly making false accusations will constitute a violation of this code and will be investigated accordingly.

The Company will protect any member or associate who raises a concern honestly

It is a violation of the Code to knowingly make a false accusation, lie to investigators, or interfere or refuse to cooperate with a Code investigation.

ANNEXURES

NO BUSINESS IS COMPLETE

... unless the forms are filled in triplicate!

ANNEXURE I

Policy on Prevention of Sexual Harassment at Workplace

1. This Policy shall be known as “Prevention of Sexual Harassment at Workplace”. This Policy has been prepared in line with the directives and guidelines set out by the Supreme Court of Bangladesh in Writ Petition No. 5916 of 2008.

2. This Policy shall be applicable to all Members to whom the Code is applicable.

3. DEFINITION:

3.1“Sexual harassment” includes

a. Unwelcome sexually determined behaviour (whether directly or by implication) as physical contact and advances;

b. Attempts or efforts to establish physical relation having sexual implication by abuse of administrative, authoritative or professional powers;

c. Sexually coloured verbal representation;

d. Demand or request for sexual favours;

e. Showing pornography;

f. Sexually coloured remark or gesture;

g. Indecent gesture, teasing through abusive language, stalking, joking having sexual implication.

h. Insult through letters, telephone calls, cell phone calls, SMS, pottering, notice, cartoon, writing on bench, chair, table, notice boards, walls of office, factory, classroom, washroom having sexual implication.

i. Taking still or video photographs for the purpose of blackmailing and character assassination;

j. Preventing participation in sports, cultural, organizational and academic activities on the ground of sex and/or for the purpose of sexual harassment;

k. Making love proposal and exerting pressure or posing threats in case of refusal to love proposal;

l. Attempt to establish sexual relation by intimidation, deception o false assurance

m. Any other unwelcome physical, verbal or non-verbal conduct of sexual nature;

n. The following circumstances may be deemed as sexual harassment, if it occurs or is present in relation to or connected with any act or behaviour of sexual harassment as defined above;

i. implied or explicit promise of preferential treatment in his / her employment /association; or

ii. implied or explicit threat of detrimental treatment in his / her employment /association; or

iii. implied or explicit threat about his / her present or future employment status / association status; or

iv. interferes with his / her work or creating an intimidating or offensive or hostile work environment for him / her; or

v. humiliating treatment likely to affect his / her health or safety.

Unwelcome is the key in defining Sexual Harassment. It will always be decided by the recipient basis the impact and effect of the behaviour.

3.2“Workplace” means -

(a) any premises that is owned or controlled by the Company; it shall include company provided transportation

3.3“Unwelcome” is the key in defining sexual harassment. It is the impact and effect of the behaviour, to the disapproval of the recipient that will define the behaviour as sexual harassment.

3.4“Relationship” implies association between two individuals out of their free will or choice as companions beyond and outside the requirements of work / profession

3.5“Consensual Relationship” refers to intimate and close relationship between two individuals perceived to be with the consent of each other. This policy will not take cognizance of complaints from concerned members to adjudicate on such relationships as a sexual harassment issue. However, should such relationships manifest as ‘conflict of interest’ situation, Company reserves its right to proceed against the concerned Members as per the disciplinary proceedings under the Code of Conduct, as appropriate.

3.6“Aggrieved Person” means a person who alleges to have been subjected to any act of sexual harassment in any workplace;

3.7“Chairperson” means Chairperson of the Prevention of Sexual Harassment Committee (PoSHC);

4. Every case of harassment is not sexual harassment. It is the impact, effect and sexual motive of the alleged behaviour / conduct, on the victim that determines the extent and gravity of sexual harassment. Inability or reluctance of the victim to raise a sexual harassment complaint due to fear or threat of job loss or disadvantage at work and / or social stigma, will not amount to acquiescence and it will not absolve the accused from charges of sexual harassment.

We consider sexual harassment to be a gender neutral issue and accordingly a sexual harassment complaint can be made either by a man or a woman if he or she has suffered a behaviour or victimisation as spelt out above.

5. No Member shall be subject to sexual harassment at any workplace;

6. It is expected that members should be conscious and be aware of behaviours that are likely to cause discomfort to the other gender and should abstain from the same. To ensure awareness of all members on this issue the Company shall hold half-yearly orientation which will be mandatory for all members. All members shall be provided and shall keep with them for ready reference the booklet provided by the Company along with this Code of Conduct. Accordingly, irrespective of the intent, motive or the extent of proximity or friendship, the following behaviours could be perceived as sexual harassment.

- Friendship gestures suggesting intimacy, like grabbing, brushing, touching, pinching, putting the arm around the shoulder / waist, etc.
- Increments, Promotions, employment benefits offered to a person on a 'quid pro quo' basis with an underlying expectation of sexual gratification e.g. asking for a night out, etc.
- Passing comments with sexual connotations, making sexist remarks, vulgar descriptions around the looks, appearance, dressing sense etc. to the embarrassment of the concerned person.
- Showing or displaying any sexually explicit visual material, in the form of pictures / cartoons / pin-ups / calendars / screen savers on computers / any offensive written material / pornographic e-mails/inappropriate sms / Whats app messages etc.
- Engaging in any other unwelcome conduct of a sexual nature, which could be verbal, or even non- verbal, like staring to make the other person uncomfortable, making offensive gesture e.g. making kissing noise, etc.
- Exhibitionism (flashing oneself) intentionally with a sexual innuendo.
- Demanding and persistently asking a person out when the person asked out is reluctant and has showed lack of interest.
- Vitiating the work environment with any of the above behaviour, since it is not objected to or has been accepted over a period of time, thereby making it hostile for the employees in general.
- A hostile work environment can also be caused by any two members in an intimate personal relationship, if the behaviour displayed by the two members created difficulties or discomfort for others. It then becomes a 'hostile work environment' for the other members.
- Unsolicited remarks, rumours and gossip casting aspersions on the character of a person attributing his / her career aspirations to intimate or quid-pro-quo relationship at work.

7. Raising Sexual Harassment Complaints

In case of any issues of sexual harassment nature, whether existing or perceived, either explicit or implied as per Section 3.1 above, the Aggrieved Person (or any other person on his / her behalf including family members, relatives, lawyer) is required to report the matter as early as possible - not later than 3 months, unless it is a case of ongoing harassment - to any of the following, without any order of preference -

1. Write to any Member of POSH Committee at their designated E Mail ID or by post;
2. Submit a written complaint in the complaint drop box made available at all locations of the Company;
3. Write to the HR representative or approach for guidance / support on raising the issue
4. Inform the Supervisor, (in case the complaint is not against him / her)
5. Write to any Member of CCC at their designated E Mail ID.
6. Email your query or complaint at - speakupmarico@ethicshelpline.in

Irrespective of the channel of communication, all reported matters (raised under 2-6) shall be duly forwarded to the PoSH Committee, within 3 days and not later than 7 days, for further action in the matter.

While there is no prescribed format for raising a complaint, it is recommended that the complainant shall make the complaint, along with necessary facts, documentary evidences and details of witnesses, as available for a thorough and unbiased inquiry into the matter.

8. Conciliation

While an Aggrieved Person has a right to raise a sexual harassment issue and get the matter investigated till its resolution, if for any reason, the member decides or chooses to withdraw the complaint - for reasons of social stigma or other personal reasons, the same shall be considered in accordance with the provisions of the law, and shall be dealt with as follows:

8.1 PoSH Committee may before initiating an investigation and at the request of the Aggrieved Person take steps to settle the matter between such Aggrieved Person and the respondent through conciliation.

8.2 No monetary settlement shall be made as a basis of conciliation

8.3 Where a settlement has been arrived at under clause 8.1 above, PoSH committee shall record the settlement so arrived and forward the same along with recommended action, to CCC to take action as specified in the recommendation.

8.4 PoSH Committee shall provide copies of the settlement as recorded by the committee to the Aggrieved Person and the respondent.

8.5 Where a settlement is arrived at, no further investigation shall be conducted by PoSH Committee.

9. INVESTIGATION

9.1 Issues raised under this policy shall be referred for investigation by the PoSH committee as defined this Code of Conduct.

9.2 The PoSH Committee shall follow the principles of natural justice by adhering to the following steps in particular with regard to inquiry into the complaint.

(i) On receipt of the complaint, the PoSH Committee will send a copy of the complaint to the accused Member, within 7 (seven) working days, indicating the deadline by which a response, along with evidences and details of witnesses should be submitted.

(ii) The accused Member shall also be given an opportunity to be heard and make written submissions on the allegations made and circumstances leading to the complaint.

(iii) In case of failure on the part of the Member to respond to the complaint or make himself / herself available for the hearing, the PoSH committee in its discretion may terminate the inquiry in favour of the victim, after giving 15 days' notice to the parties concerned.

(v) The parties will be entitled to engage a lawyer to represent their case in proceedings before the PoSH committee.

At the recommendation of the PoSH committee, choice of location and additional witnesses as per the requirement of the victim may be considered. Details of the investigation are "Privileged and confidential" and the PoSH committee shall determine the people (including audit) and the content of findings to be made available - for the purposes of reporting to the management.

9.3 In case of conciliation as per clause 8.1, PoSH is authorised to conduct independent investigation, in case the terms and conditions of the settlement has not been complied with by the respondent.

9.4 In the event, the victim chooses to take recourse to law, the company may at its sole discretion decide to not pursue the matter further.

9.5 Investigation shall be completed within a period of period thirty (30) days which may be extended upto sixty (60) days where necessary

9.6 During the pendency of an investigation and for the safety of the Aggrieved Person, on a written request made by the Aggrieved Person, PoSHC, may recommend to the Company -

a) Suspension of the Respondent or transfer of the Respondent / Aggrieved Person to any other workplace; or

b) grant paid leave to the Aggrieved Person upto a period of three months; or

c) grant such other reasonable relief to the Aggrieved Person as may be directed by the PoSH Committee - viz.

• a restraint on the accused Member to oversee / supervise the work performance of the victim in case of direct working relationship;

• assigning the performance evaluation to another supervisor at the discretion of the management;

• Any other relief as appropriate.

9.7 The leave granted to the Aggrieved Person as above, shall be in addition to the leave he / she would be otherwise entitled.

10. Investigation Report

10.1 Investigation report along with its finding and recommendation shall be submitted to the PoSH Committee and PoSH Committee will submit the same to CCC within a period of ten days from the date of completion of the investigation in consideration of the following -

(i) Nature of evidences in support of the allegation;

(ii) Leading circumstances culminating into sexual harassment;

(iii) Discrepancies, if any, in the allegations and the submission made by the victim and his / her witnesses;

(iv) Grounds for review or counter allegations/ evidences from the accused.

(v) In preparing its report the PoSH Committee shall take both Oral and Circumstantial evidence into account

10.2 In case the PoSH Committee arrives at the conclusion that the allegation against the respondent has not been proved, it shall recommend to CCC that no action is required to be taken against the respondent. However, in case the complaint is found to false, malicious, and frivolous then such complaining Member shall be liable for disciplinary actions, including but not limited to payment of compensation to the respondent.

10.3 In case the PoSH Committee arrives at the conclusion that the allegations against the respondent has been proved, it shall recommend to the CCC as the case may be

i) to take action for sexual harassment as a misconduct in accordance with the provisions of the Code;

ii) The punishment could range from warning, monetary penalty and counselling to termination of employment depending on the gravity of the offense and its impact on the victim.

iii) In case of monetary fine or penalty, the PoSH may recommend for the same to be paid to the victim to defer the cost of medical treatment or for seeking professional counselling, as the situation may warrant and for this purpose, the Company is authorised to make requisite recoveries from the remuneration payable to the accused and in case of separation of the employee, for such recoveries to be made out of the final settlement.

iv) CCC shall act upon the recommendations of PoSH committee within thirty days of receipt of final investigation report.

11. Determination of Compensation to Aggrieved Person

For the purpose of clause (iii) of 10 above, in determining the sums to be paid to the Aggrieved Person, PoSH shall have regard to -

a) the mental trauma, pain, suffering and emotional distress caused to the Aggrieved Person

b) the loss in the career opportunity due to the incident of sexual harassment

c) medical expenses incurred by the Aggrieved Person for physical and psychiatric treatment

d) the income and financial status of the respondent

e) feasibility of such payment in lump sum or in instalments.

The Company shall have the right to withhold the dues equivalent to the awarded compensation from any dues payable by the Company to the Respondent by way of remuneration/ final settlement.

12. Powers of PoSHC

12.1 For the purpose of investigation, the PoSH committee shall have the following powers:

12.1.1 Summoning and enforcing the attendance of any Member and examining such Member

12.1.2 Requiring the discovery and production of documents; and

12.1.3 Any other matter which may be prescribed.

13. Appeals And Revision

The decision of the CCC is final and shall not be open to any review or appeal, unless additional evidences not considered by the PoSH Committee are brought on record or fresh instances emanating from past sexual harassment complaint have arisen.

The CCC in such cases may order a fresh investigation and the matter will be re-opened and pursued as an independent investigation without prejudice to the findings and recommendations of the PoSH committee,

14. Members of Prevention of Sexual Harassment (PoSH) Committee

A designated and independent committee known as PoSH Committee will be set up, constituting the Internal Complaints Committee for the purposes of dealing with sexual harassment complaints, pursuant to this Policy.

The PoSHC must at all times have a minimum of 5 (five) members, majority of whom will be female. At least 2(two) members of the Committee shall be external members not within the employment of the Company and shall be chosen out of a panel of persons having experience/expertise in gender/sexual harassment matters. The PoSHC shall be Chaired by a female.

The CCC shall monitor and oversee the working of the PoSH committee in addition to ensuring that the constitution of the PoSH Committee shall at all times conform with the requirement of the Guidelines and Directives of the Supreme Court of Bangladesh.

15. Training and Communication

The PoSH committee will steer a robust communication and awareness building program across the organization by undertaking the following -

i) Display of the details of the PoSH Committee members along with contact details, reporting mechanism and the PoSH policy at conspicuous places in all locations

ii) Include a module on Sexual harassment in the corporate training programs including induction courses

iii) Conduct specialised capability building training programs for members of the PoSH committee

iv) Make available evidences of attendance / confirmation on training for audit verification

v) Maintain necessary log and provide details of sexual harassment complaints.

ANNEXURE II

A. Members of Code of Conduct Committee (CCC)

Sr.No	Committee Member	Designation	Email Id
1	Siddharth Das	Director - HR	sidhartha.das@marico.com
2	Md. Iqbal Cowdhury	Chief Financial Officer	iqbal.chowdhury@marico.com
3	Christabel Randolph	Head-Legal & Company Secretary	christabel.randolph@marico.com

The Chief Financial Officer shall act as the Chairperson of the CCC and the Head-Legal shall act as the Secretary of the CCC

B. Members of Prevention of Sexual Harassment Committee (PoSHC)

As defined under clause 14 of the PoSH policy.

Sr.No	Committee Member	Designation	Email Id
1	Siddharth Das	Director - HR	sidhartha.das@marico.com
2	Christabel Randolph	Head-Legal & Company Secretary	christabel.randolph@marico.com
3	Saiful Alam	Head-Manufacturing	saiful.alam@marico.com
4	Shruti Ambegaoker*	Head-OD, Marico Limited	Shruti.Ambegaoker@marico.com
5	External Member		

ANNEXURE III

MBL'S CODE OF BUSINESS ETHICS (MCOBE)

This code is applicable to all our associates.

Associate means external person/body of persons / company / organisation MBL does its business with. They could be advertising agencies, distributors, consultants, vendors, suppliers, third party manufacturers, etc.

1.Ethics

To meet social responsibilities, you are expected to conduct your business in an ethical manner and act with integrity.

You shall safeguard and make only appropriate use as authorized by MBL Group of confidential information and ensure that all employees, associates, business partners privacy and valid intellectual property rights are protected.

2. Legal Compliance

a) You will comply with all the applicable laws, regulations, rules and regulatory orders.

b) You will acquire appropriate knowledge of the requirements relating to your duties sufficient to enable you to recognise potential dangers and to know when to seek advice from Legal department of MBL on specific law or company policies and procedures.

c) Violation of any law, regulations, rules and orders may make you liable for criminal or civil action, in addition to termination / suspension of your association with the company without any compensation / damages for such action against you.

d) You will not at any time or under any circumstances enter into an agreement or understanding, written or oral, express or implied with any competitor concerning prices, discounts, other terms or conditions of sale, profit or profit margins, costs, allocation of products or geographic markets, allocation of customers, limitations on production, boycotts of customer or suppliers, or bids or the intent to bid or even discuss or exchange information on these subjects. These prohibitions are absolute and strict observance is required.

3. Prohibition of Corruption & Bribery

You warrant that you will not make any payment, gift or other commitment to Members of MBL group, to Government officials or otherwise in a manner contrary to applicable laws, policies or standards of conduct, for the purpose of obtaining or facilitating the performance of or otherwise relating to the contract.

Nothing in this Policy will render MBL liable to reimburse the vendor / associate / agents or their associates for any such consideration given or promised or for any consequences arising out of such actions.

4 Labour and Human Rights

You shall comply with all laws including specifically, the labour laws. In case of any discrepancy between MBL's understanding or interpretation of law and yours, please note that for decision on violation of this Code, MBL's interpretation of law shall apply.

You will ensure that the work environment provided by you to your employees / staff is free from all types of harassment.

You will not use any form of forced, bonded or child labour. You are expected to protect the human rights of your employees / staff and to treat them with dignity and respect.

5. Health & safety of the employees / staff

You will provide a safe and healthy working environment for all the employees / staff working at your office / factory.

6. Environment Protection

It is essential that you will have to comply with all applicable environmental regulations. All required / applicable permits, licenses, information registrations and restrictions shall be obtained by you.

ANNEXURE IV

TABLE 0F CONTENTS

Information Security Policy

ANNEXURE IV

Information Security Policy

1. Introduction

1.1 This Policy shall form part of each Member's terms of employment / association along with the appointment letter issued to or the agreement entered into with him / her.

1.2 The Company is committed to protecting the confidentiality of personal information relating to the Members. The Members understand and agree that certain personal information is required by the Company for operational purpose and have accepted to let the Company have access and the right to use such information.

1.3 The Company is committed to the protection of the information assets and information technology resources that support its operations globally. The Company's scale of operations necessitates exchange and transmission of humungous information, sensitive or otherwise, electronic or otherwise on a day to day basis.

1.4 Without the implementation of appropriate controls and security measures, these resources are subject to potential damage or compromise to confidentiality or privacy, and thus disrupting the activities of the Company as well as of individual Member.

1.5 The purpose of this Policy is to maintain, secure, and ensure legal and appropriate use of the Company's information technology infrastructure. The Company's policy seeks to place security and privacy policy specifics in service of each other in order to provide Members with a high quality, trusted and secure computing environment, and as a means of protecting and securing its assets interests, data and intellectual property.

1.6 This Policy shall substitute previous Policy(ies) pertaining to Information security.

2. Title and Objective

2.1 This Policy shall be called as "Information Security Policy". Herein after to be referred to as "the IT Policy"

2.2 The obligations set out under the IT Policy are mandatory and shall be enforceable between the Company and for Member/s.

2.3 Objective of the IT Policy

2.3.1 to prevent unauthorized disclosure of information

2.3.2 to prevent unauthorized, deliberate alteration of information

2.3.3 to prevent unauthorized, deliberate destruction or deletion of information and prevent practices which obstruct or degrade the usability of the information technology resources

2.3.4 safeguard against situations wherein the Company could incur legal liabilities due to unacceptable actions of its Members

2.3.5 to comply with all applicable regulatory and legislative requirement

2.4 Members shall:

2.4.1 keep themselves abreast of the physical security and authentication rules in accessing the information systems authorized for use

2.4.2 adopt additional vigilant security practices while using mobile devices (like Laptops, Smart Phone, mobile phones etc)

2.4.3 secure individual passwords and not sharing them

2.4.4 use the facility for the Company business purposes only

2.4.5 restrict instant messaging only for the Company business purpose and not to send / receive text / audio / video file to any other person

2.4.6 use centralized file share facilities to store data where possible, and limit copies on local storage / removable media

2.4.7 not download content / software / material indiscriminately from unknown sources / restricted / abandoned site either directly or indirectly through the Company's IP address without express permission / approval from the Head-Commercial & Business Process Transformation.

3. Definitions

3.1 In this Policy, unless the context otherwise requires:

3.1.1 "Access", with its grammatical variations and cognate expressions means gaining entry into, instructing or communicating with the logical arithmetical or memory function resources of a computer, computer system or computer network

3.1.2 "Applicable Law(s) / Law" includes any laws laid down by a Competent legislature, decisions of Judicial form having a binding effect and national or international treaties that have a binding effect

3.1.3 "Associate" means a Person who or which has access to or use of, either directly or indirectly, the Computer Resource of the Company and includes consultant, contractor, supplier, vendor, distributor, third party manufacturer, any other business associate by whatsoever name called

3.1.4 "Confidential or Proprietary information" shall have same meaning as defined in terms of employment or association

3.1.5 "Communication" means dissemination, transmission, carriage of information or signal in some manner and includes both a direct communication and an indirect communication

3.1.6 "Company asset" includes Company owned information, Data, Device, Information system, Computer Network, Computer System, Computer Resource

3.1.7 "Computer" means any electronic, magnetic, optical or other data processing device or system which performs logical, arithmetic and memory functions by manipulations of electronic, magnetic or optical impulses and includes all input, output, processing, storage, computer software or communication facilities which are connected or related to computer in a computer system or computer network;

3.1.8 "Computer network" means the interconnection of one or more computers through -

(i) the use of satellite, microwave, terrestrial line or other communication media; and

(ii) terminals or a complex consisting of two or more interconnected computers whether or not the interconnection is continuously maintained

3.1.9 “Computer resource” means Computer, Computer System, Computer Network, Data, computer data base or software

3.1.10 “Computer system” means a Device, including input and output support Devices and excluding calculators which are not programmable and capable of being used in conjunction with external files, which contain computer programmes, electronic instructions, input data and output data, that performs logic, arithmetic, data storage and retrieval, communication control and other functions

3.1.11 “Data” means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the Computer

3.1.12 “Device” means any electronic, electromechanical, electro magnetic optical or other instrument, machine or component, equipment or apparatus which is used or can be used, whether by itself in combination with any other instrument and computer system, to view or to inspect or to listen to or record or transmit any information or data and includes a collection of devices

3.1.13 “Grievance Officer” means Head – Commercial & Business Process Transformation.

3.1.14 “HOD” means Head of Department, by whatever designation known

3.1.15 “Information” includes data, text, images, sound, voice, codes, computer programmes, software and database or micro film or computer generated micro fiche

3.1.16 “Information system” means all hardware and software assets of MBL that store, process or transmits data / information of the Company and includes servers, email, SAP, MI-Net and other applications, programs, desktops, laptops, network elements like routers, switches, firewalls

3.1.17 “IT personnel” includes a Member entrusted with the responsibility of developing, maintaining and safe guarding Information Technology systems and solutions for the Company

3.1.18 “Joint Venture” means a contractual arrangement whereby two or more parties undertake an economic activity, which is subject to joint control

3.1.19 “Member” means a person who is -

1. an employee whether part-time or full-time, fixed term, permanent trainee; or
2. an individual who is a temporary staff, intern, secondee, an apprentice; or
3. a third party or parties who represent the Company or act on behalf of the Company; or
4. an employee of Joint Ventures where the Company has management control; or
5. an employee of new acquisitions; or
6. an Associate

3.1.20 “Official purpose” means the purpose for which any information, data or computer resource is provided to a Member in furtherance of fulfilment of his / her professional commitment towards the Company

3.1.21 “Person” includes an individual, any company or association or body of persons, whether incorporated or not

3.1.22 “Personal device” means any device which is not provided by the Company

3.1.23 “Parent Company and/or Subsidiary” shall have same meaning as defined under the Companies Act 1994

3.1.24 “SOP” means Standard Operating Procedures

3.1.25 “Virus” means a program that has the capability to spread by replicating itself to destroy, damage, degrade or adversely affect the performance of the computer resource that requires some user action to trigger it off

3.1.26 “Virtual Private Network (VPN)” means a network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to the Company’s computer network

3.1.27 “Worm” means a program that has the capability to spread by replicating itself to destroy, damage, degrade or adversely affect the performance of the Computer Resource that propagates in accordance with its own inbuilt logic without any action from the user.

3.2 Interpretation:

3.2.1 Save to the extent that the context or the express provisions of this Policy otherwise require:

3.2.1.1 headings and sub-headings are for ease of reference only and shall not be taken into consideration in the interpretation or construction of this Policy;

3.2.1.2 all references to clauses and Annexure are references to clauses of, Annexure to this Policy;

3.2.1.3 Annexures to this Policy are an integral part of this Policy and reference to this Policy includes reference thereto and reference to any Annexure includes reference to any Annexure or Appendix thereto;

3.2.1.4 any reference in this Policy to any law or any provision thereof shall, in relation to an area in which such law or such provision is not in force, be construed as a reference to the corresponding law or the relevant provision of the corresponding law, if any, in force in that area;

3.2.1.5 words importing the singular include the plural and vice versa;

3.2.1.6 words importing a particular gender include all genders;

3.2.1.7 the term “including” means including but without limitation;

3.2.1.8 expression in the present time shall mean a reference also to the past or future timeand vice versa;

4. Commencement, Applicability and Breach

4.1This Policy shall come into force with immediate effect upon adoption.

4.2 Applicability:

4.2.1 This Policy is applicable to all the Members.

4.2.2 To the extent this Policy conflicts with Applicable Law, the Applicable Law shall prevail.

4.3 The obligations set out under this Policy are mandatory.

4.4 Breach of any of the obligations, by a Member shall invoke the penalty and indemnity clauses as contained in the Policy.

In the event of any notice of non-compliance under this Policy, the burden of proof of compliance shall be that of the Member.

5. Modifications To The Policy

5.1 MBL reserves the right to modify these guidelines from time to time. Any changes to this Policy shall be duly communicated to all Members through appropriate channels and would be effective and shall be binding on the Members.

6. Guidelines for Providing Suggestions on this Policy

6.1 If any Member has any doubts about this Policy or wishes to make any comments or suggestions regarding these guidelines, you can email us at infosecurity@maricoindia.net or contact: Mr. Gaurav Sarda, Head-Commercial & Business Process Transformation (Grievance Officer).

7. General Restriction

7.1 Any Device including any personal Device or Device which is provided by the Company, which is, or has been, engaged in any Communication with or without attachment(s) in respect of any Company information and / or Data; in course of employment or association with the Company will be deemed to be Company asset.

7.2 It is hereby clarified that any Communication through such Device whether such communication is made during office hours or otherwise and / or on a holiday or on working day will be deemed to be made for "official purpose".

7.3 The Company shall have the right to access, copy, share, transfer, remove, and delete, all Information / Data on Device that is used by a Member for official purpose.

The individual waives his right to privacy in respect of any personal data including photos / files etc stored on the device.

8. Responsibilities of Members

8.1 Member should read, understand and comply with this Policy.

8.2 Member may make a requisition for Company asset only in the form specified in Annexure I if such Company asset is required to carry out the entrusted functions. The Member should clearly mention the purpose for the usage of the Company asset. Such form needs to be approved by HOD of respective departments.

8.3 Laptop may be provided to a Member in Manager grade and above or to a Member in any other grade, after approval from their respective HOD & Head-Commercial & Business Process Transformation.

8.4 All Members will follow a standard Computer configuration Policy as provided by the Company across the globe. Any deviation in this configuration will require approval of respective MD.

8.5 Member will be able to get a replacement of existing laptop only after defined period, Currently 4 years through proper approval process. After 4 years, laptop reaches "Technical End of life" and also becomes un-manageable in terms of getting spare / support.

8.6 Members shall hand over the laptop computer at the end of its technical life to the company.

8.7 Member should ensure that they are aware of, and understand, the security procedures for the specific Computer Systems they use.

8.8 Member should take all reasonable precautions to protect Information Systems against unauthorized access, use, disclosure, modification, duplication or destruction of computer, Computer Network, Computer System, Device, Information System.

8.9 Member should use Information Systems only as may be necessary for their job responsibilities.

8.10 Member should use available mechanism and procedures to protect their own Data and Data under their control.

8.11 Member should take back up of critical information and data in the desktop / laptop regularly at least once a week using company provided software.

8.11 Member should assist and co-operate in the protection of the Computer Systems they use.

8.12 Member should use Information Systems in compliance with Applicable Laws relating to electronic activity, confidentiality, copyrights, licenses and contractual obligations.

8.13 Member should report security problems / threats or issues to respective supervisors, systems administrator or help desk as may be appropriate.

8.14 Member should make an entry of information (like machine and adaptor serial number) of temporarily issued laptops in ''Gate Pass Card for Issuing Portable Assets'' at the time of entry to and exit from the offices of the Company. The form is enclosed in Annexure II.

8.15 The Members shall be solely responsible for the physical security of the devices provided by the company. In the event of loss of Laptop Computers other than due to the negligence of the Members, the Company shall provide a replacement, loss of Laptop Computers more than one shall be deemed to have been caused due to Member negligence. Save and accept the above, loss of all Devices shall be replaced by the Member at his cost.

8.16 Member should ensure that the desktop provided to him / her is handled with proper care. To shift the desktops, Member need to log a call with local helpdesk, who will co-ordinate with Admin Department for shifting the Desktop.

8.17 On separation from the services / association of / with Marico, Members should submit to the IT department email Member-ids, application Member-ids, materials, software, hardware, desktop / laptops etc that have been provided to the Member to carry out his / her job.

9. Policy Pertaining to Electronic Mail

9.1 Members shall be provided with access to computing resources through any Device shared or for exclusive use depending upon the nature of work and level of the Member in the Company.

9.2 Members shall be provided with official email address with permission to receive and send internal and external mail.

9.3 Mail and Mailbox size on mail server shall be decided by the Head-Commercial & Business Process Transformation from time to time and communicated to the Members. Request for relaxation of mailbox size shall be considered Head-Commercial & Business Process Transformation, subject to approval by the HOD.

9.4 All temporarily associated Members will be provided with email ids to send internal mail on request from HOD of relevant department. Permission to send external mail will be given on recommendation by concerned department to IT.

9.5 The Company may monitor, inspect, disclose the content of any Member in the business interests; or required under any law or order of the Court or any Statutory authority(ies); or when there is reasonable ground to believe that Information Security Policy is being violated, or have been violated.

9.6 Any deviation to this Policy will require written or email authorization from such Member's HOD and HR HOD.

9.7 Acceptable Use:

9.7.1 Email is permitted primarily for official purposes with limited personal use only. It is however advisable that personal email ids be used for non official mail.

9.7.2 Use of official email ids for subscription to newsgroups, interest groups, social networking sites, blogging sites or any mode of communication through internet will be strictly as per provisions of this Policy. This does not include sites initiated by the Company namely Kwench, TSR Darashaw etc. Official email ids can be given to Banks / finance companies etc. for enabling transactions. Official Email ids can also be used for receiving communications on topics related to official business.

9.7.3 No Communication for official purposes shall be routed through any means other than through Company provided Devices, Computer Resources, Computer Networks, Email Addresses. In case any personal email id is required to send mail in cases of emergency, this use shall be reported to the HOD within 3 days. This relaxation shall not apply to any person serving notice period.

9.8 Unacceptable Use:

9.8.1 Transmitting internal, confidential, proprietary communication without permission or authority.

9.8.2 Personal use which can interfere with the Company's computing resources or cause irritation, inconvenience to the recipients or other Members.

9.8.3 Mass mailers or chain initiation / forwarding i.e sending or forwarding of any non business email to more than 2 individual recipients or any group id outside the Company is prohibited.

9.8.4 Sending emails in excess of the email size shall be prohibited.

9.8.5 Use of another Member's email account without express written permission.

9.8.6 Impersonating or concealing one's identity.

9.8.7 Revealing password to any other person.

9.8.8 Use of email id in online mail groups, blogs etc without permission of HOD.

9.8.9 Sending messages or viewing content which is offensive, discriminatory, inflammatory or defamatory about individual, group or organization, race, gender, religion, national origin, attributes or sexual preferences.

9.8.10 Viewing / Sending messages containing any obscene, indecent or porno graphic material.

9.8.11 Use of services such as Dropbox, Yousendit or any other file sending software or cloud based storage for the purposes of business communications.

10.Policy For Internet Usage

10.1 Company provides for centralized internet facility to Members for official purpose

10.2 Company may impose reasonable restrictions in respect of timings, duration, sites etc in the best interests of the Members and Company.

10.3 Acceptable Use

10.3.1 Browsing sites or search engines for business related work and furthering the knowledge in areas of expertise

10.3.2 Limited use for internet banking

10.3.3 Limited personal use.

10.4 Unacceptable Use

10.4.1 Unauthorized access / entry into any third party or Company's Computer System

10.4.2 Activity resulting in disruption to third party or Company operations

10.4.3 Playing online games, viewing or transmitting sexually explicit content, hacking, gambling or any such activity which is illegal and prohibited under applicable law(s)

10.4.4 Downloading software without permission of the Head-Commercial & Business Process Transformation.

If any software is required for better productivity or for any official purpose, then Member may send a written or email request to the IT helpdesk. The IT team will evaluate whether the required software is safe to install and if found safe, IT will install it. Such software will be added to the safe software list of IT so that software can be installed in future without need for evaluation process. This list will be reviewed by IT department every year or on receipt of any information that such software can be rendered unsafe.

10.4.5 Posting confidential, proprietary information either of Company or any third party on social networking sites, groups, blogs etc.

10.4.6 Viewing / Sending fraudulent or obscene or messages designed to inconvenience others.

10.4.7 Sending messages or viewing content which is offensive, discriminatory, inflammatory or defamatory about any person. This is in relation to race, religion, national origin, attributes or sexual preferences.

10.5 Internet Privacy

10.5.1 Usage of Internet via Company's computer Network is not confidential

10.5.2 All accesses to internet will be logged. These logs will be viewed by authorized IT personnel. These can also be shared with the concerned HOD or HR. Logs can also be shared with law enforcement authorities when called upon to do so.

Usage of internet via company's computer network is not confidential and will be logged. The logs can be shared with concerned HOD or HR or law enforcement authorities if required.

10.6 Blogging & Use of Social Networking Sites

10.6.1 All blogs except for official blogs should carry the following disclaimer "The views expressed are personal and do not reflect views of the author's Employer".

10.6.2 Members shall use appropriate language for such blogging / micro sites, social network platforms. Such language should not hurt any person, class of persons or society's sentiments.

10.5.3 Any official blogs can be posted after obtaining written or email authorisation of the MD, Head-Legal and Investor Relations Dept.

11.Dial-in Access ("VPN") Policy

11.1 Members can use VPN connections to gain access to the Company's computer network from the outside. VPN access should be strictly controlled, using one-time password authentication as far as practicable.

11.2 It is the responsibility of Member with VPN access privileges to ensure that a VPN connection is not used by any non-Member to gain access to the Company's information system. A Member who is granted VPN access privileges must remain constantly aware that VPN connection between his/her location and the Company is literal extension of the Company's computer network, and that they provide a potential path to the Company's information. Member must take every reasonable measure to protect Company assets.

11.3 Subject to clause 15, analog and non-GSM digital cellular phones cannot be used to connect to Company's Computer Network, as their signals can be readily scanned and / or hijacked by unauthorized individuals. Only GSM & CDMA standard digital cellular phones are considered secure enough for connection to Company's Computer Network.

11.4 Dial in access account activity shall be monitored, and if a VPN account is not used for a period of six months the account will expire and no longer function. If dial-in access is subsequently required, the Member may request a new account in the manner prescribed.

11.6 Acceptable Use

11.6.1 Members shall keep domain password confidential.

11.6.2 Members shall have installed antivirus & its latest updates onto their Computer before using VPN.

11.6.3 Member shall not access the Company's Computer Network over VPN unless the Device used by the Member to access contains latest anti-virus programme.

11.6.4 Members shall not download / save / store any data on devices other than those that are Company provided.

11.7 Unacceptable Use

11.7.1 Members shall not save passwords in the phone book of the dial-up adaptor.

11.7.3 Members shall be careful to log out from the Computer on completion of the work.

12.Protection Of Information

12.1 Virus Protection

12.1.1 Company provides for various Antivirus agents for protection of computer system; currently McAfee is installed in all the computer systems to protect the system from Virus, Trojans, Logic bombs or any such unwanted programs. A firewall is installed at the perimeter of HO & all data centres connected via internet to protect internal network from hackers.

12.1.2 Acceptable Use:

12.1.2.1 Members should ensure that his / her desktops or laptops are configured with the standard anti-virus or any other security software that is used within the Company. This also applies to company provided or financed mobile devices.

12.1.2.2 Members should scan floppies, CD-ROMs or any plug & play data storage drive for viruses if any before connecting them to the system in the network.

12.1.2.3 Members should report virus attacks if any, to the system administrator along with the necessary details like name of the virus, the action taken and the results thereon.

12.1.2.4 All software should be installed with help of IT Infrastructure team only.

12.1.3 Unacceptable Use:

12.1.3.1 Members should not attempt to modify the configuration of the anti-virus installed on their desktops or laptops.

12.1.3.2 Members should not bring Floppies, CDs or any plug & play data storage drives from unknown sources

12.1.3.3 Members should not download or install any shareware or freeware on the Company's Computer systems.

12.1.3.4 Members should not connect computer systems to the Company's computer network without latest updated Antivirus installed.

12.1.3.5 Members should not install any software on his / her own on the system.

12.2 Securing Data on Desktop/ Laptop Computers

12.2.1 All Computer Systems are pre-installed with backup agent for centralised data backup of Desktops / Laptop's onto the data backup server.

12.2.2 Acceptable Use:

12.2.2.1 Member's mail files, .pst files must be password protected and should be stored in email folder in the root of the drive.

12.2.2.2 Members should lock screen with passwords that activate after 3 minutes of inactivity. The screen should go blank after this period.

12.2.2.3 Members should keep their important data in a folder named "My data" or "My Documents" & .pst files in "Emails" folder in the root of the C or D drive.

12.2.2.4 Members should take back up of all important Data before travelling. If travel is for an extended duration i.e for more than 10 days, it is advisable to take a complete backup of the Data on to Computers

12.2.2.5 If Member's laptop Computer is lost, Member must immediately notify the nearest police station as well as the Company's Systems Manager, and give them specific information to identify their laptop Computer.

12.2.3 Unacceptable Use:

12.2.3.1 Members should not leave printouts of sensitive information unattended.

12.2.3.2 Members shall not share directories over the Computer Network without password protection and specific Member-level access;

12.2.3.3 Members shall not tamper with or attempt to modify the registry on Windows based systems.

12.2.3.4 Members should not leave laptops unattended in public places.

12.3 Clear Desk and Clear Screen Policy

12.3.1 Members are provided with a workstation having drawers with lock & key. External storage Devices are provided on request received from respective Member's HOD / Supervisor.

12.3.2 Acceptable Use:

12.3.2.1 Members shall take adequate precautions to protect the confidentiality and integrity of Confidential and Internal information that they deal with or that is made available to them.

12.3.2.2 Members shall protect files and other papers (non-electronic format) that contain sensitive or confidential information from unauthorized access.

12.3.2.3 If a confidential documents need to be printed, Members are advised to use password protected print outs. The SOP for the same is available onMera Milaap.

12.3.2.4 Members shall ensure that unwanted printed paper containing confidential / sensitive information should be disposed off completely (Shredded), and all efforts should be made by Members to ensure confidentiality of the data being destroyed.

12.3.2.5 Members shall lock their workstation when idle.

12.3.2.6 When receiving sensitive faxes Members must be physically present to receive the same.

12.3.2.7 When transmitting sensitive faxes, Members are advised to inform the recipient of the fax first before transmission.

12.3.2.8 Members shall format the removable disk drives when the documents in it are not needed anymore.

12.3.3 Unacceptable Use:

12.3.3.1 Members should not leave any printouts unattended

12.3.3.2 Members shall not keep files & folders unattended.

12.4 Password Use

12.4.1 Passwords help in maintaining confidentiality of data and restricting access to authorized Members. Members are provided passwords to gain access to applications such as SAP, Email, Intranet and other applications.

12.4.1 Acceptable Use:

12.4.1.1 Members should use work group passwords solely within the Members of the group.

12.4.1.2 Members should keep passwords confidential.

12.4.1.3 Members should select and change their own passwords.

12.4.1.4 Members should change all Computer System-level passwords (e.g. root, enable, NT admin, application administration accounts, etc.) every month.

12.4.1.5 Members should change all Member-level passwords (e.g., email, web, desktop computer, etc.) at least every 45 days.

12.4.1.6 Members should conform passwords implemented on server level to the following:

12.4.1.6.1 The passwords should be at least 8 characters in length.

12.4.1.6.2 Password must include alphabets, numbers and must contain a special character.

12.4.1.6.3 Passwords must not contain dictionary words.

12.4.2 Unacceptable Use:

12.4.2.1 Members shall not use obvious and easily guessable passwords.

12.4.2.2 Members shall not store passwords on computer system in an unprotected form / clear text.

12.4.2.3 Members shall not reveal passwords to others.

12.5 Safe Disposal of information storage devices

12.5.1 Members should adhere to the following:

12.5.1.1 Be attentive when handling Device that will be disposed of.

12.5.1.2 For disposal of hard disk, pen drives, they must be formatted multiple times and low level formatting of hard disks must be ensured before disposal.

12.5.1.3 CD ROM and DVDs must be broken before disposal. Manual destruction or shredders may be used for the same if available.

12.5.2 Members shall not dispose external disk drives without following proper process as provided by the Company.

13.Laptop/desktop Usage Policy

13.1 Members shall maintain the integrity and prohibit misuse of device, computers, peripherals and other related resources that may be provided by the Company.

13.2 Acceptable Use:

13.2.1 Members shall consider the Computer and its related peripherals (mouse / monitor / keyboard / external storage Devices etc.) assigned for official purpose and should not swap with any Computer within or outside their departments.

The Member should take good care of their assigned Devices.

13.2.2 Members shall maintain the identity of computers by not tampering with the asset ID and vendors Serial No. (E.g. Toshiba / IBM / HP etc). Member shall inform the IT department in the event of these labels not available on their machines.

13.2.3 It is recommended that temporary files on computers shall always be deleted on a regular basis as this utilizes a lot of disk space and can slow down the performance of the computer. Members must take help from IT support person for doing the same, if required.

13.2.4 Member must lock his desktop / laptop (Ctrl+Alt+Del+Enter) while leaving the desk for extended periods of time.

13.2.5 Important files must be encrypted / password protected and placed on separate disk partition other than partition on which the Operating System is installed.

13.2.6 Members are discouraged to share their folders as a normal practice. If at all it is required then the Members may share the folders in “READ only” mode and if required passwords protect them.

13.2.7 Guest Account on Computer Network must be disabled by default and Members shall not be enabling it under any circumstances.

13.2.8 Administrator account must be renamed and must have strong password as laid down by the password policies.

13.2.9 Screen savers with password shall be used to protect the machine from unauthorized access.

13.3 Unacceptable Use:

13.3.1 Members shall not change the basic input output settings as configured by IT dept. on their computers.

13.3.2 Members shall not use objectionable wallpaper on the device provided to them by the Company.

13.3.3 Members shall not under any circumstances change the hostname or IP address of their Computers.

13.3.4 Members shall not use the "administrator" Member account for logging on to the Computer System.

13.3.5 Members should not tamper or dismantle their workstation, Desktops and Laptop Computer or any Devices attached with the computer systems.

13.3.6 Members should not attach any personal Devices with the computer like pen-drive, external HDD, CD writer, floppy drive or any other storage Device including iPods. In case Member wants to do it for some business purpose then it should be approved in writing by HOD / Head - IT.

13.3.7 Members should not allow visitors / guest to connect their laptop / any Device with the Company's Computer Network.

13.3.8 Members can connect only Devices which are provided by the Company for official purpose

14. Software Usage, Maintenance and Monitoring

14.1 Members shall ensure proper utilization of software used at the Company's Computer System and Computer Network and to control unapproved / unauthorized software usage.

14.2 Acceptable Use:

14.2.1 Members shall request for installation of new software by any employee must have an approval from his / her reporting manager and must have a valid license.

14.2.2 Members shall be aware that Head-Commercial & Business Process Transformation reserves the right to seek justification from any Member for installation of any particular software and may suggest alternate software in best interest of the Company.

14.2.3 Members shall not install software on devices provided by the Company (like music players, chatting messengers etc.) Devices are handled by IT support and they must be informed if any changes are required to be carried out.

14.2.4 Members must ensure that antivirus patches and windows updates are applied on a regular basis (Once in every 15 days).

14.2.5 Members shall not override, disable or change configuration of Windows updates or antivirus updates.

14.2.6 Members shall disable the macros in case a file that is received contains macros that they are unsure about.

15. Wireless Communication Policy

15.1 This part of Policy prohibits access to the Company's Computer Networks via unsecured wireless Communication mechanisms.

15.2 This part of Policy is applicable to all wireless Communication Devices connected to any of the Company's Computer Network. This includes any form of wireless Communication Device capable of transmitting packet data. Wireless Devices and / or Networks without any connectivity to the Company's Network do not fall under the purview of this Policy.

15.2 Register Access Points And Cards

15.2.1 All wireless access points / base / stations connected to the Company's Computer Network must be registered and approved by the IT department. These access points / base stations are subject to periodic penetration tests and audits. All wireless Network Interface Cards used in corporate laptop or desktop computers must be registered with the IT department.

15.3 Approved Technology

15.3.1 All wireless LAN access must use Company-approved vendor products and security configurations.

15.4 VPN Encryption And Authentication

15.4.1 All Computers with wireless LAN Devices must utilize a Company-approved VPN configured appropriately to prevent unauthorized access into the Company's Computer Network. To comply with this Policy, wireless implementations must maintain point to point hardware encryption of at least 128 bits. All implementations must support a hardware address that can be registered and tracked, i.e., MAC address. All implementations must support and employ strong Member authentication.

15.4.2 All gateways / routers acting as base stations / wireless hotspots should be configured to log all terminals connected to / through it and the logs should be stored for a minimum period of three months unless specified otherwise specified by any law for the time being in force.

15.4.3 Use of unsecured wifi such as those found in airports / coffee shops is allowed only if used along with VPN. This is because any hacker can eavesdrop and gain access to your computer

15.5 Setting The Service Set Identification (SSID)

15.5.1 The SSID should be configured so that it does not contain any identifying information about the organization, such as the Company name, division title, employee name, or product identifier.

15.5.2 The SSID key must use strong cryptographic controls and be set to WPA-PSK authentication at a minimum.

15.5.3 This facility will be configured and made available only by IT personnel and none other.

16. Due Diligence Measures

16.1 Members shall not view, create, host, display, upload, modify, publish, transmit, update or share any information that —

16.1.1 belongs to another person and to which the Member does not have any right

16.1.2 is harmful, harassing, blasphemous, defamatory

16.1.3 obscene, pornographic, paedophilic, libellous, invasive of another's privacy, hateful, or racially, ethnically objectionable, disparaging, relating or encouraging money laundering or gambling, or otherwise unlawful in any manner whatever

16.1.4 harms minors in any way

16.1.5 infringes any patent, trademark, copyright or other proprietary rights

16.1.6 violates any Applicable Law for the time being in force

16.1.7 Deceives or misleads the addressee about the origin of such messages or communicates any information which is grossly offensive or menacing in nature

16.1.8 impersonates another person

16.1.9 contains software viruses or any other Computer code, files or programs designed to interrupt, destroy or limit the functionality of any Computer Resource;

16.1.10 threatens the unity, integrity, defence, security or sovereignty of Bangladesh, friendly relations with foreign states, or public order or causes incitement to the commission of any cognizable offence or prevents investigation of any offence or is insulting any other nation.

16.2 The Company shall remove any Information or Data specified in clause (2) above or Communication link to any such Information or Data within 36 (thirty-six) hours of such Information, Data or Communication link coming to the actual knowledge of the Company;

16.3 The Company may preserve such information as is specified in clause 2 above and associated records for at least 90 (ninety) days for investigation purposes;

16.4 The Company may appoint and keep appointed at all times a Grievance Officer to provide information or any assistance to Government agencies who are lawfully authorised for investigative and protective cyber security activity, on a request in writing stating clearly the purpose of seeking such Information or any such assistance.

16.5 At no time shall the Company knowingly deploy or install or modify the technical configuration of any Computer Resource or become party to any such act which may change or has the potential to change the normal course of operation of the Computer Resource than what it is supposed to perform, thereby circumventing any law for the time being in force, except where such technological means is developed, produced, distributed or employed for the sole purpose of performing the acts of securing the Computer Resource and Information contained therein.

16.6 The name and contact details of the Head-Commercial & Business Process Transformation appointed under this Policy shall be published on the Company's corporate website.

16.7 The mechanism by which Members or any victim who suffers as a result of access or usage of IT Devices by any person in violation of clause 2 of these due diligence measures can notify their complaints against such access which may be made publicly available and published on the Company's corporate website.

16.8 The Head-Commercial & Business Process Transformation shall ensure that it will redress all complaints made under this Policy; within one month from the date of receipt of complaint.

17. Indemnity By Members

17.1 The Member shall hereby indemnify and agrees to keep indemnified Marico from or against any loss, damage, demand, claim, penalty, liability including but not limited to third party claims, that are lodged on the Company and that may arise statutorily or otherwise with regard to the breach, non-compliance, mal compliance, part compliance of the obligations of the Member as stated in this Policy.

18 .Enforcement

18.1 Members are encouraged to report any improper activity to CCC. All decisions of the Head-Commercial & Business Process Transformation shall be taken in consultation with the Head-HR and shall be final and binding. The Head-Commercial & Business Process Transformation shall report to the MD on matters under this IT Policy.

18.2 Anonymity and Confidentiality

18.2.1 When a Member reports any grievance to the Grievance Officer through any medium, such Member may choose to remain anonymous, although Members are encouraged to identify himself / herself to facilitate communication and investigation.

18.2.2 If Member makes his / her identity known, the Grievance Officer and investigators will take every reasonable precaution to keep such Member's identity confidential.

18.3 Members have multiple options to reach the Grievance Officer to report any grievances / post any query / concern. Member may choose to reach out to multiple Members in the Company who shall be equipped to help such Member resolve concern:

1. Line management
2. Line HR Manager
3. Any Member of the Code of Conduct Committee.

18.4 Investigations

18.4.1 The procedures for handling potential violations of this Policy have been developed to ensure consistency in the process across the organization. Within this framework, Company will ensure it follows local grievance procedures, if any specified by the local laws and investigations will be conducted by the Grievance Officer and Head-HR.

18.4.2 While conducting an Investigation following any complaint, the Company will ensure it adheres to the Principles of natural justice namely:

18.4.2.1 Both parties shall be given reasonable opportunity to be heard along with witnesses and to produce any other relevant documents

18.4.2.2 No Person will be allowed to be a judge in his / her own case

18.4.2.3 The final decision will be made after due investigation and the application of proper reasoning

18.4.2.4 The order of the investigations team shall be in writing and shall contain reasons for arriving at the decision

18.4.3 The decision of the investigations team may be published on the Company's corporate website.

18.5 Compliance

The Head-Commercial & Business Process Transformation shall be responsible to submit ay every quarter a report, of all incidents/grievances reported to the CCC, to the MD and Compliance Officer or Company Secretary of the Company.

19 . Penalty

19.1 Non-compliance or violation of this Policy will result in disciplinary action against the Member as may be decided by the CCC upon recommendation of the Grievance Officer and Head-HR and shall include termination.

19.2 The penalty for negligent non-compliance of the Policy for the second instance will be reprimand which may be permanently noted in the personnel records of the relevant persons and additionally, the performance allowance and / or other allowances or incentives of the relevant persons may be temporarily / permanently withheld as per the sole discretion of the CCC.

19.3 The penalty for subsequent negligent non-compliance of the Policy shall be termination from employment followed by arbitration proceedings to determine damages. The sole arbitrator shall be appointed by the CCC.

19.4 In case of willful and deliberate non compliance of this Policy, the employment of the non-compliant Member or association of the non-compliant Member shall be liable to be terminated without any compensation.

19.5 Additionally, if no financial loss is caused by the willful and deliberate non compliance, a nominal penalty may be imposed at the sole discretion of the CCC

19.6 In case financial loss is caused by the willful and deliberate non compliance, then the CCC shall determine damages if any.

19.7 It may be noted that none of the above preclude the Company from filing criminal complaints, before the appropriate legal authorities, against the persons who have negligently or deliberately breached the provisions of this Policy.

19.8 Notwithstanding anything contained above, the CCC will decide on the penalty commensurate with the gravity of the breach.

19.9 Notwithstanding anything stated herein, the Company may take legal action (Civil / criminal) against the Member for violation of this Policy or Applicable Law.

20 . Severability

If any provision of this Policy is or becomes illegal, invalid or unenforceable, such provision shall be severed and the remaining provisions shall continue unaffected.

21 . Amendment

This Policy can be amended by the Company at its discretion. The CCC shall notify any amendments to the policy to the members or on the Corporate Website inviting comments and suggestions. The Company may after considering the comments and suggestions may make suitable further amendments. Such further amendments, if any, shall come into force immediately with effect from the date of such notification of the amendment.

22. Affirmation Of Acceptance And Acknowledgement:

Each Member should affirm acceptance of MBL's Information Security Policy through a declaration that should read as prescribed below:

I have received and read MBL's Information Systems Security Policy.

I understand the matters contained therein that there may be additional policies / guidelines or laws specific to my role.

I agree to comply with the MBL's Information Security Policies and Guidelines in spirit and letter.

I shall:

a) keep myself abreast of the physical security and authentication rules in accessing the information systems authorized for use;
b) adopt additional vigilant security practices while using mobile devices like (Laptops, Smart Phone, mobile phones etc);
c) secure passwords and not share them;
d) use the facility of the Company for the Company's business purposes only;
e) restrict instant messaging only for the Company business purpose and not to send/receive text / audio / video file to any other person;
f) use centralized file share facilities to store data where possible, and limit copies on local storage / removable media.
g) not download and / or install any type of content / software / material either directly or indirectly through Company's IP address or otherwise onto Computer system without express permission or approval from IT Committee.

Signed_____

Name_____

Type of Association (tick which ever is appropriate)
Employee / Trainee / Associate / Consultant / Retainer / Contractor / Vendor / Supplier / Distributor / Apprentice
(if any other, specify): _____

Date_____

Appendix I

Systems Asset Requisition Form

Date of Request:	Name of the Member:s
Location:	Emp. No.:
Division/Department:	Floor/Block (if applicable):
Grade:	Extn No:
Requisition For:	
Purpose:	
Benefits:	
Name of HOD:	
Name of MD:	
Signature of the Member:	

* Above information will be used to prepare the CEP, if required.

For System Use:	
Request received date:	
Request accepted / rejected:	
Please mention the alternatives explored to meet the Member request:	
Is the required asset available in working condition to meet the mentioned requirement? If not, what is the cost of the requested asset?	
Through what resource will the requested asset be procured?	
Date action initiated on:	Expected completion date:
CEP reference no., if any:	PO reference no., if any:
Name of the Authorizing Systems Person:	
Signature of Systems Person:	

Appendix II

Gate Pass Card for Issuing Portable Assets

(to be retained with security personnel) G.P. Sl.

Name of the Member: Emp. No.:	Division/Department: Location:
Machine Sl. No.: Adapter Sl. No.:	MBL Asset No.: Insurance Policy No.:
Make: Model:	Configuration:
Type of Asset (please tick): ☐ Capital Item ☐ Loan Item ☐ Vendor Standby Item ☐	
Date of issue: Authorized by (Name): Designation:	Date: Signature:

Date	Time Out	Receiver's Name & Signature	Security's Signature	Date	Time in	Depositor's Name & Signature	Security Signature	Remarks/Purpose of issue

This item is the sole property of MBL. This item is provided to me for the official use and I am fully accountable for any theft/damage/loss.

Marico Bangladesh Limited has all rights to question me or recover money from me for the portable asset issued to me in the event of loss/theft/damage. I will return the company's asset issued to me at the time of transfer, separation or on demand. While I am in office I will keep the asset in lock and key if not in use.

Name of the Member & Signature: Date :

(to be retained by the HR& Administration Dept) G.P. Sl.

Name of the Member: Emp. No.:	Division/Department: Location:
Machine Sl. No.: Adapter Sl. No.:	MBL Asset No.: Insurance Policy No.:
Make: Model:	Configuration:
Type of Asset (please tick): ☐ Capital Item ☐ Loan Item ☐ Vendor Standby Item ☐	
Date of issue: Authorized by (Name): Designation:	Date: Signature:

Date	Time Out	Receiver's Name & Signature	Security's Signature	Date	Time in	Depositor's Name & Signature	Security Signature of issue	Remarks/Purpose

Appendix III

Data Protection Policy

1. Introduction

Data Protection Policy for the Company ("DPP") sets out commitment of MBL to protect the privacy and integrity of sensitive personal data or information (defined later) collected by the Company.

2. Objective:

2.1 To ensure that data is collected and used fairly and lawfully

2.2 To process personal sensitive data or information only in order to meet its operational needs or fulfill legal requirements

2.3 To establish appropriate retention periods for personal sensitive data or information

2.4 To ensure that Members' rights can be appropriately exercised

2.5 To provide adequate security measures to protect personal sensitive data or information

2.6 To ensure that queries about data protection, internal and external to the organization, is dealt with effectively and promptly

2.7 To regularly reviewing data protection procedures and guidelines within the organization.

3. Applicability

3.1 The Company collects various information / data from its Members / associates ("provider of such information") which may be classified as:-

1) Financial information
2) Sensitive Personal information
3) Physical health information
4) Medical history
5) Biometric information.

3.2 This information is requested by the Company at the time of joining / association. Further, personal information and sensitive personal information ("such information") / data are requested under a lawful contract.

4. Definitions

4.1 "Data" means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner and is intended to be processed, is being processed or has been processed in a computer system or computer network and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer;

4.2 "Information" includes data, text, images, sound, voice, codes, computer programmes, software and database or micro film or computer generated micro fiche;

4.3 "Personal information" means any information that related to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person;

4.4 "Sensitive personal data or information (SPDI)" of a person means such personal information which consists of information relating to:

i) password;
ii) financial information such as Bank account or credit card or debit card or other payment instrument details ;
iii) physical, physiological and mental health condition;
iv) sexual orientation;
v) medical records and history;
vi) Biometric information;
vii) any detail relating to the above clauses as provided to body corporate for providing service; and
viii) any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise:

Provided that, any information that is freely available or accessible in public domain or furnished under the law relating to Right to Information or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these rules.

5. Purpose For Collecting Sensitive Personal Information

5.1 MBL collects sensitive personal information from its Members / associates for the purposes:

5.1.1 Biometric information is collected in order to provide uninterrupted ingress and egress in the MBL's premises

5.1.2 Financial information viz. TIN, Bank Account details, etc. are collected in order to direct credit any financial emolument to provider of such information

5.1.3 Medical history is collected in order to check the Health status.

6. MBL's Responsibility

6.1 MBL to obtain "Consent Form" [Appendix III (A)] from the provider of such information

6.2 MBL will not use / disseminate / disclose such information except for the purpose for which such information was collected. (To be read with point no.8)

6.3 MBL to provide privacy guidelines for handling of or dealing in such information including sensitive data or information;

6.4 MBL to request such information only under a lawful contract with the provider of such information and not otherwise;

6.5 However, MBL should not be held responsible pertaining to the authenticity of the personal information or sensitive personal information

6.6 MBL to ensure that such information is available for view by such provider of information who has provided such information under lawful contract

6.7 MBL shall publish such privacy guidelines on its website http://marico.com/bangladesh

6.8 MBL will provide access to such information to the provider of such information as and when request is received from the provider of such information.

6.9 MBL will keep such information secure as provided under the Applicable Laws

6.10 MBL will address any discrepancies and grievances of provider of such information with respect to processing of information in a time bound manner.

6.11 MBL has designated Head-Commercial & Business Process Transformation as it's Grievance Officer.

6.12 Grievance Officer to redress such grievance within one month from the date of receipt of grievance.

7. Rights of Provider of such Information

7.1 Right to review - Provider of SPDI will have right to review such Information they had provide and ensure that any such information found to be inaccurate or deficient shall be corrected or amended as feasible.

7.2 Right to not to provide such information - Provider of SPDI shall be within his / her rights to deny providing of such Information to MBL, however, if such information is not provided then Company will be within its rights to deny any facility / service for which such information was sought.

7.3 Right to withdraw - Provider of SPDI will have an option to withdraw consent given earlier to MBL. Such withdrawal of consent to be sent in writing to MBL. MBL will be within its rights to deny any facility / service for which such information was sought.

8. Disclosure of such Information

8.1 Company will not use / disseminate / disclose such information except for the purpose for which such information was collected.

8.2 Company shall require permission from the provider of such information prior to disclosing such information to any third party.

8.3 Company will not require any prior permission from provider of such information when such information is to be shared / disclosed with Government / Governmental agencies mandated under law to obtain such information for the purpose of verification of identity or for prevention, detection, investigation including cyber incidents, prosecution and punishment of offences.

8.4 Notwithstanding anything contained in point 8.1 and 8.2 above, such information shall be disclosed to any third party by an order under the law for the time being in force

8.5 Company or any person in its behalf will not publish such information.

Appendix III (A)

Format of Consent Form

Personal / Sensitive Information Consent Form

Name of Member:

Employee Code:

Please Read Carefully, Complete and sign this form.

The Information and Communications Technology Act, 200 and rules made there under mandates that consent be obtained prior to the collection and use of all personal / sensitive information.

The personal / sensitive information you provide to Marico will be used for the purposes reasonably associated with the employment / association.

"Sensitive personal data or information (SPDI) of a person means such personal information which consists of information relating to:

1. password;
2. financial information such as Bank account or credit card or debit card or other payment instrument details ;
3. physical, physiological and mental health condition;
4. sexual orientation;
5. medical records and history;
6. Biometric information;
7. any detail relating to the above clauses as provided to body corporate for providing service; and
8. any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise:

Provided that, any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2009 or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these rules."

Please specify from the above the type of personal / sensitive data or information that you are providing to the Company

_____

These purposes include direct credit of salary, incentive amount / bonus, etc. and uninterrupted ingress / egress in the office premises by use of Biometric identification.

Additional personal information may be collected from time to time. Consent for the use of this personal / sensitive information may be inferred where its uses are obvious and it has been voluntarily provided.

Complete text of the Data Protection Policy for MBL (variously the "Policy" or "Policies") may be found at www.marico.com/bangladesh

Should a Member wish to review their personal information held by MBL, they must make a request to the MBL pursuant to that MBL's Policy.

Further, Member may withdraw consent to use their personal / sensitive information pursuant to the Policies. Such a withdrawal however, may require the cancellation of your employment/ association with or suspension or modification of your activities with MBL.

All Members must sign a copy of this form.

I hereby consent to the receipt, collection, storage and use by the Company of all Sensitive Personal Data or Information that I have hitherto provided or May hereafter provide.

_____

Signature of Member

Date:

ANNEXURE V

TABLE OF CONTENTS

ANNEXURE V

Introduction

Insider Trading is not only unethical and immoral but indeed illegal as it fuels illegitimate speculation in the share prices on the Stock Exchanges. Such a profiteering by insiders by misusing confidential information available to them by virtue of their position or connection with the Company erodes investors' confidence in the integrity of the management of a Company.

The Securities and Exchange Commission (SEC) issued the Insider Trading Rules 1995 which governs the law relating to insider trading and protection of unpublished price sensitive information in Bangladesh governs the law relating to insider trading and protection of unpublished price sensitive information in Bangladesh. These Regulations have been amended since then from time to time. The updated SEC Regulations can be obtained from the SEC website http://www.secbd.org/. The Company will readily provide a copy of the same upon request of any member.

Employees, Directors and their relatives and other persons connected to the Company, on the basis of unpublished price sensitive information which may impact the price of the security, thereby making a profit or avoiding a gain.

In line with the SEC Insider Regulations, MBL Share Dealing Rules for Employees were originally framed and adopted by the Board of Directors of the Company on October 29, 1999. Further, these Rules were amended form time to time as under:

- MBL Employees (Dealing in Securities and Prevention of Insider Trading) Rules, 2002 approved by the Board of Directors of the Company on April 18, 2002 superseded the originally framed Rules of 1999.
- MBL Employees (Dealing in Securities & Prevention of Insider Trading) Rules, 2009 approved by the Board of Directors of the Company on January 22, 2009 superseded the Rules of 2002.
- MBL Employees (Dealing in Securities & Prevention of Insider Trading) Rules, 2012 approved by the Board of Directors of the Company on May 3, 2012 superseded the Rules of 2009.

MBL Employees (Dealing in Securities & Prevention of Insider Trading) Rules, 2012 are further amended by the Board of Directors of the Company on January 31, 2014.

These Rules are embedded in MBL's Unified Code of Conduct.

Code of Corporate Disclosure Practices for Prevention of Insider Trading

1.0 Corporate Disclosure Policy

1.1 To ensure timely and adequate disclosure of price sensitive information, the following norms shall be followed by listed companies:

2.0 Prompt disclosure of price sensitive information

2.1 Price sensitive information shall be given by listed companies to stock exchanges and disseminated on a continuous and immediate basis.

2.2 Listed companies may also consider ways of supplementing information released to stock exchanges by improving Investor access to their public announcements.

3.0 Overseeing and co-ordinating disclosure

3.1 Listed companies shall designate a senior official (such as compliance officer) to oversee corporate disclosure.

3.2 This official shall be responsible for ensuring that the company complies with continuous disclosure requirements. Overseeing and co-ordinating disclosure of price sensitive information to stock exchanges, analysts, shareholders and media and educating staff on disclosure policies and procedure.

3.3 Information disclosure/dissemination may normally be approved in advance by the official designated for the purpose.

3.4 If information is accidentally disclosed without prior approval, the person responsible may inform the designated officer immediately, even if the information is not considered price sensitive.

4.0 Responding to market rumours

4.1 Listed companies shall have clearly laid down procedures for responding to any queries or requests for verification of market rumours by exchanges.

4.2 The official designated for corporate disclosure shall be responsible for deciding whether a public announcement is necessary for verifying or denying rumours and then making the disclosure.

5.0 Timely Reporting of shareholdings / ownership and changes in ownership

5.1 Disclosure of shareholdings / ownership by major shareholders and disclosure of changes in ownership as provided under any Regulations made under the Act and the listing agreement shall be made in a timely and adequate manner.

Disclosure/ dissemination of Price Sensitive Information with special reference to Analysts, Institutional Investors

6.0 Listed companies should follow the guidelines given hereunder while dealing with analysts and institutional investors:

(i) Only Public information to be provided - Listed companies shall provide only public information to the analyst / research persons/large investors like institutions. Alternatively, the information given to the analyst should be simultaneously made public at the earliest.

111

ACKNOWLEDGMENT / CONSENT FORM

ACKNOWLEDGMENT / CONSENT FORM

Affirmation of acceptance and acknowledgement:
Each Member shall affirm acceptance of this Code through declaration that shall read as prescribed below:

For new Joinees:
I have received and read MBL's Unified Code of Conduct for Members with its Annexures. I understand the matters contained in the Code and understand that there may be additional policies or laws specific to my role. I agree to comply with the Code in spirit and letter.

Signed_____
Name_____
Date_____

Quarterly Affirmation
I have complied with this Code during the Quarter _____

Signed_____
Name_____
Date_____

MBL Ltd.

Phone: 022-6648-0500

For feedback, queries, suggestions, please write to speakupMBL@ethicshelpline.in